United States District Court

NORTHERN DISTRICT OF TEXAS

In the Matter of the Search of
(Name, address or Brief description of person, property or premises to be searched)

Yahoo, an Internet Service Provider located at
701 First Ave., Sunnyvale, California 94089

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 3:07-MJ-459

I Greg Christiansen **being duly sworn depose and say:**

I am a(n) Special Agent with the U.S. Immigration and Customs Enforcement (ICE) **and have reason to believe that** XX_ **on the property or premises known as** (name, description and/or location)

(SEE ATTACHMENT A).

in the NORTHERN **District of** TEXAS **there is now concealed a certain person or property, namely** (describe the person or property to be seized)

(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed,

concerning a violation of Title 18 **United States code, Section(s)** 500 and 513. **The facts to support a finding of Probable Cause are as follows:**

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT GREG CHRISTIANSEN)

Continued on the attached sheet and made a part hereof. XX **Yes** _ **No**

Signature of Affiant
GREG CHRISTIANSEN
Special Agent, ICE

Sworn to before me, and subscribed in my presence

October 10, 2007 @ 2:50 PM
Date

at Dallas, Texas
City and State

PAUL D. STICKNEY
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is Yahoo, an Internet Service Provider, located at 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized, constituting evidence, fruits, and instrumentalities of violations of Title 18, United States Code § 500, Counterfeit Money Orders, and § 513, Counterfeit Securities of the States and Private Entities, are as follows:

1. Any and all Yahoo accounts for henrysaunders2004@yahoo.co.uk, to include all email, histories, buddy lists, profiles, subscriber information, method of payment, and detailed billings records (log on & log off times).

2. All customer or subscriber account information for the subscriber(s) to henrysaunders2004@yahoo.co.uk, including any e-mail address(es) and all customer or subscriber account information for any additional accounts subscribed to by the same subscriber(s) as henrysaunders2004@yahoo.co.uk. For each such account or e-mail address, the information should include the subscriber's name, account, login name, address, telephone number or numbers, and any other information pertaining to the identity of the subscriber, including any billing information;

3. User connection logs for all accounts identified in paragraph 1 above from May 16, 2007, to the present date. User connection logs should contain connection time and date, disconnect time and date, method of connection to system, and data transfer volume; and

4. The contents of all messages including instant messages, e-mail messages and attachments, including all messages sent to or from the accounts identified in paragraph 1 at any time after May 16, 2007.

STATE OF TEXAS)
)
COUNTY OF DALLAS)

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Greg Christiansen (Affiant), currently a Special Agent with U.S. Immigration and Customs Enforcement, being duly sworn, depose and state that:

I am a Special Agent (SA) with the Department of Homeland Security, U.S. Immigration and Customs Enforcement ("ICE"), assigned to the Special Agent in Charge (SAC) in Dallas, Texas. I have been so employed with ICE and the former Immigration and Naturalization Service for the past eleven years. As part of my duties as an ICE agent, I have experience in narcotics, money laundering, and fraud criminal investigations. I have testified before federal grand juries and federal district courts in Texas. I have received formal training in the areas of smuggling, narcotics, money laundering, and fraud. During my years as a law enforcement officer, I have had substantial experience in conducting various types of investigations. This experience includes the use of surveillance, undercover recordings, search warrants, development of informants and other intelligence gathering techniques related to the investigation of smuggling, narcotics, money laundering, and fraud.

PURPOSE OF AFFIDAVIT

This affidavit sets forth facts, and suggests reasonable inferences from those facts, establishing that there is probable cause to believe that evidence of continuing violations of Title 18, United States Code § 500, counterfeit money orders, and § 513, counterfeit Securities of the States and private entities, will be found in the accounts and records of Yahoo, an Internet Service Provider ("ISP"), located at 701 First Avenue, Sunnyvale, California, relating to the email account of henrysaunders2004@yahoo.co.uk. Yahoo is a commercial electronic

communication service company that provides its subscribers electronic mail (email) services.

The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and agencies, including inspectors with the Department of Homeland Security, U. S. Customs and Border Protection or other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

On the basis of the entire contents of this Affidavit, Affiant believes there is probable cause for the issuance of a search warrant for the premises described in Attachment "A" for the purpose of seizure of physical evidence described in Attachment "B" related to the offenses of possession of counterfeit instruments.

THE INTERNET IN GENERAL

The Internet is a world-wide network of computer networks. A network is a system of interconnected computer systems and terminals. This connectivity allows data to be stored and exchanged between computers remotely. Every computer on the Internet has a unique address, like a telephone number, represented by a string of numbers separated by periods. This address is called an Internet Protocol (IP) address. It is this IP address which allows information to travel across the Internet and be delivered to the correct computer.

Different aspects of the Internet are accessed or used by applications which allow users to access, transmit, and exchange information. These applications include the World Wide Web (WWW or www) and email. The WWW allows users to display and access data in a multimedia format. Email is a method for exchanging electronic correspondence or other information

between computer users enabling users to communicate by computer similar to writing letters and sending them through normal mail.

A software application, called a browser, such as Microsoft Explorer or Netscape Navigator, is used to display World Wide Web multimedia information known as web pages or web sites. Each web page on the WWW has its own unique identifier associated with an IP address. This identifier can be expressed as a series of alphanumeric strings separated by periods such as www.fbi.gov and is called a Uniform Resource Locator (URL). In order to access any web page on the WWW or in broader terms, the Internet, a browser uses the URL to request, search, locate, and display the web page of interest.

URLs may be very long, but each will have a base element which is called the domain name. In the URL www.fbi.gov, the domain name is fbi.gov. Since all URLs must be unique, all domain names on the Internet are governed by the Domain Name System (DNS) which is managed by a non-profit corporation called the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names can then be purchased and registered through companies known as registrars who process new domain name requests with ICANN.

An individual or group can then obtain a unique domain name by contacting a registrar and requesting it. If the domain name is available, the requestor enters into a registration contract with the registrar, setting forth the terms under which registration is accepted and will be maintained. Registrars collect various contact and technical information for registration from the requestor. The registrar will then keep records of the contact information and submit the technical information to a central directory known as the "registry." This registry provides other computers on the Internet the information necessary to send email or to find web sites.

As mentioned earlier, another major use of the Internet is email. By being able to

identify all Internet computers by domain name and IP addresses, emails sent over the Internet can be traced back to the original sender. Email messages contain header information which documents the route through one or more computers that the email traveled as it was sent from the originator to the receiver. The header information can contain a message identification number which is a unique identifier for each specific message, as well as the date, time, and time zone when the message was sent. The route is documented in the header using IP addresses of each computer that the message passed through. This header information can be used to determine and trace the email message route which can ultimately lead to identifying the actual origination point for the email.

STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

This application is made pursuant to Federal Rule of Criminal Procedure Rule 41, Search and Seizure, and Title 18, United States Code, Sections 2703(a), (b) and (c). Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access." This statute was amended following the events of September 11, 2001 by The Patriot Act, which became effective October 26, 2001. All statutory references are to the amended statute which took effect October 26, 2001, relevant parts of which are set forth for the Court's convenience.

A. Title 18, United States code, Section 2703(a) provides:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only **pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means

available under subsection (b) of this section.

B. Title 18, United States Code, Section 2703(b) provides, in part:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection–

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued **using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant. . .

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service–

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

C. Title 18, United States Code, Section 2703(c) provides, in part:

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity–

(A) **obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant**. . . .

D. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter–

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

E. Title 18, United States Code, Section 2510, provides, in part:

(8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

(14) "electronic communications system" means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .
(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications; . . .
(17) "electronic storage" means –
(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

STATEMENT OF PROBABLE CAUSE

1. On July 26, 2006, United States Magistrate Judge Paul Stickney, Northern District of Texas, issued an anticipatory search warrant for the premises of 4500 Sojourn Rd., Apt. #2303, Addison, Texas 75001, the residence of Ana C. Logan, to conduct a search for violations of Title 18, United States Code § 500, Counterfeit Money Orders, and § 513, Counterfeit Securities of the States and Private Entities.

2. On July 27, 2006, Special Agents with ICE, including Affiant, executed the search warrant. During the search, ICE agents found 913 American Express Traveler's Checks, 316 U.S. Postal Money Orders and $300 dollars in cash, all within three different Federal Express (Fed-Ex) packages. Affiant obtained verification that the traveler's checks and money orders were indeed counterfeit.

3. The Fed-Ex packages were from Accra, Ghana and were addressed to Ana Logan. Logan, who resides alone at 4500 Sojourn Rd., Apt. #2303, was present during the search and agreed to be interviewed.

4. Logan made the following statements to Affiant:

a. she did not know that the monetary instruments were counterfeit.

b. on or about June 28, 2006, Logan received an email titled "JOB OFFER FOR

YOU". The content of the email is as follows: "Hello, Are you interested in a part time job?i have a job offer for you,check out my website www.henrysaunderstextilesandfabricscompany.org/EMPLOYMENT.htm."

c. on or about June 28, 2006, Logan responded to the email titled "JOB OFFER FOR YOU" and was later contacted by email by someone known to Logan as Henry Saunders with the email address of henrysaunders01.aim.com.

d. via email, Saunders offered Logan a job forwarding checks to people throughout the United States by utilizing Fed-Ex and completing the appropriate Fed-Ex forms.

e. on or about July 5th, 2006, Logan began receiving Fed Ex packages from someone identified as Henry Saunders.

f. Logan's typical work for Henry Saunders involved receiving Fed-Ex packages, at first containing sealed preaddressed brown envelopes, and then sending the envelopes to their final destination via Fed-Ex through the United States, as instructed by Saunders via email and Instant Messaging. The second Fed-Ex package from Saunders contained loose U.S. Postal Money Orders. Both by email and instant message, Saunders directed Logan to complete the money orders with the names and addresses that were provided by Saunders and to send the money orders to those addresses in the United States. She was paid $100 for the first package and $300 for the second.

5. On July 28, 2006, Saunders instructed Logan by instant message to send six (6) American Express Traveler's Checks via Fed-Ex to Wayne Qualls, at the address of 3602 Birch Drive, Irving, Texas 75060, using the Fed-Ex account number of Carol Miranda, purportedly one

Drive, Irving, Texas 75060, using the Fed-Ex account number of Carol Miranda, purportedly one of Saunders' business associates.

6. On August 2, 2006, United States Magistrate Judge Paul Stickney, Northern District of Texas, issued an anticipatory search warrant for the premises of 3602 Birch Drive, Irving, Texas 75060, to conduct a search for violations of Title 18, United States Code § 513, Counterfeit Securities of the States and Private Entities.

7. On August 3, 2006 Special Agents with ICE, including Affiant, executed the search warrant. During the search, ICE agents found the original Fed-Ex package containing the six (6) counterfeit American Express Traveler's Checks and hard copies of email conversations between Qualls and an individual known only to Qualls as De Mel. De Mel utilizes a yahoo email account of demelhiranya098@yahoo.com. Qualls was present during the search and agreed to be interviewed.

8. Qualls made the following statements to Affiant:

a. Qualls received a junk email from Charles Jones (charlesjones4asimons_234@yahoo.com.mx), purportedly working for a company named Alfred Simons Textiles, which solicited people to work from home. Charles Jones wanted people to receive payments from their clients in the United States and Canada, cash the checks in their personal bank accounts, then deduct 10 percent as payment and forward the balance to the company via Money Gram or Western Union. Qualls sent a reply as requested to charles4asimons@aim.com with all of his personal information in anticipation of being hired.

b. Qualls was later contacted by email a person known to him only as De Mel,

with the email address of "demelhiranya098@yahoo.com", confirming that Qualls would be receiving checks to be cashed in his account. These checks were supposed to be from clients that owed De Mel money. Around the same time that Qualls was expecting checks to arrive, Saunders had instructed Logan to Fed-Ex the six American Express Traveler's Checks to Wayne Qualls residing at 3602 Birch Drive, Irving, TX with the Fed-Ex account number that belonged to Carol Miranda.

9. After the controlled delivery of the Fed-Ex package containing the counterfeit traveler's checks, Qualls, in cooperation with law enforcement, sent De Mel an email confirming that he had received a Fed-Ex from package from Carol Miranda containing the six traveler's checks. De Mel replied to Qualls stating that Carol Miranda worked with him and that he needed Qualls to go to his bank, deposit the checks and send the funds on that day. De Mel wanted the money sent to Elizabeth Robinson in London, UK. De Mel also added a test question for Qualls to send along with the money. The question was, "how old are you?" And the answer was 50 years.

10. On December 27, 2006, Saunders sent Logan two UPS packages from an unknown source within the United States that contained $395,000 in counterfeit American Express Traveler's Checks. Through Instant Messages, Saunders told Logan that he was preparing Fed-Ex waybills for Logan so she would be able to distribute the counterfeit monetary instruments. Saunders stated that he would be sending the Fed-Ex waybills via email.

11. Prior to January 3, 2007, all email and Instant Message communications with Henry Saunders have come from the following e-mail address: henrysaunders01@aim.com.

12. On January 3, 2007, Saunders sent Logan three emails utilizing a new email address

of henrysaundersprop@yahoo.com. The three emails contained 33 Fed-Ex waybills with 32 different names and addresses and one duplicate that were created by Saunders using the Fed-Ex website. As per Saunders' instructions, Logan was to distribute 10 counterfeit American Express Traveler's Checks in each individual package.

13. Later on January 3, 2007, Fed-Ex Senior Manager, Jeffery Tallman, of the Addison, Texas Fed-Ex facility, working in concert with Agent Christiansen, caused the Fed-Ex website to reflect that all 32 packages were shipped out by Logan, just as she was directed to do by Saunders. Because the Fed-Ex account was being used to commit fraud, the account was cancelled by the company. Since the account was cancelled and the return sender of James Smith, 619 Sequoia Dr., Colorado Spring, Colorado reflected on the waybills appeared to not exist, Fed-Ex caused its records to reflect that the packages were being held for security reasons.

14. On January 5, 2007, Saunders informed Logan that he realized that the packages were not being shipped and were being held by Fed-Ex when he checked the tracking number on fedex.com. On the same day, Saunders sent Logan another email with most of the same names and addresses that he wanted packages sent to using Fed-Ex. This time, Saunders instructed Logan to use UPS, and he provided a UPS account number (352RR6), a UPS account user name (oyigi171) and a password (babyboy).

15. On January 8, 2007, UPS Security Representative, Mark Shaffner, of the Dallas, Texas UPS facility, working in concert with Agent Christiansen, caused the UPS website to reflect that 32 packages were sent out by Logan, once again, just as Saunders directed her to do. Once again, no distribution was actually made and the UPS account was cancelled.

16. Through the actions of Fed-Ex and UPS, Logan was able to tell Saunders that she used all of the counterfeit Traveler's Checks by sending them out just as he had directed her.

Saunders would not have been aware of exactly how many counterfeit American Express Traveler's checks that Logan received, since the two original UPS packages appeared to have not come directly from Saunders.

17. On January 15, 2007, Mark Shaffner contacted Agent Christiansen about one of the intended receivers of one of the fake packages. The receiver, Allen Lee Townsend (aka: Shelemo BEN-KENNETH) of Route 2 Box 192, Luther, Oklahoma, called UPS to complain that his package had not been delivered and even offered to pay for the shipping himself. Shaffner informed Townsend that the packages had been seized by Customs Special Agent Christiansen and provided Townsend with a contact number. On that same day, Agent Christiansen was able to contact Townsend. Initially Townsend was angry because he believed that Customs and the Department of Homeland Security had no business seizing his package. After the nature of the scam was explained to him, Townsend calmed down. Townsend stated that the person he was dealing with overseas was Henry Saunders and that he was unaware that the UPS packages contained counterfeit traveler's checks. Townsend stated that he thought this was legitimate work from a type of business advertised on the junk email website that was sent to him weeks earlier. Townsend assured agent Christiansen that he would not inform Saunders about their conversation or investigation and that he would be willing to meet with an ICE Special Agent in Oklahoma City.

18. On January 18, 2007, Townsend met with ICE Special Agent Eric Munson of the RAC/OK. Townsend provided Agent Munson with all of the email conversation that he had with Saunders. Saunders was utilizing the Yahoo email account of henrysaunders2004@yahoo.co.uk. Upon receiving the checks, Saunders instructed Townsend via email to write his name and date on the topmost portion checks and to sign the checks on the

lower portion of the check in the presence of a cashier at his bank. Once the checks were cashed, Saunders wanted Townsend to deduct 10 percent. He was then to withdraw the remaining 90 percent and send that amount by Western Union to Jerry Jones in Nairobi, Kenya.

19. On January 25, 2007, United States Magistrate Judge Paul Stickney of the Northern District of Texas, issued a search warrant for the email account of henrysaunders2004@yahoo.co.uk, to conduct a search for violations of Title 18, United States Code 523, Counterfeit Securities of the States and Private Entities.

20. The Affiant executed the search warrant, and discovered the Roberta Harouff was receiving directives from Henry Saunders regarding the distribution of counterfeit monetary instruments throughout the United States.

21. On March 19, 2007, United States Magistrate Judge Nancy A. Vecchiarelli, Northern District of Ohio, issued a search warrant for the premises at 1 Windswept, Rittman, Ohio 44270, to conduct a search for violations of Title 18, United States Code 513, Counterfeit Securities of the States and Private Entities.

22. On March 20, 2007 Special Agents with ICE, including Affiant, along with the assistance of the Rittman Police Department, executed the search warrant. During the search, ICE agents discovered counterfeit monetary instruments with a face value of $537,000, Western Union receipts payable to Roberta and David Harouff from Nairobi, Kenya, lists of names and addresses for distribution of checks, and email conversations between the Harouffs and Henry Saunders.

23. Roberta and David Harouff were read their Miranda rights and agreed to waive their rights and answer questions concerning the counterfeit check scheme. Both Roberta and David Harouff admitted that they knew that the checks were counterfeit but still agreed to assist Henry

Saunders by distributing the checks throughout the United States. Roberta Harouff agreed to let Affiant take control of her identity on her Yahoo email and Instant Messenger account haroufflpn@yahoo.com and her AOL email account harouffbabe@aol.com.

24. Posing as Roberta Harouff, Affiant has maintained email and Instant Messenger (IM) contact with Henry Saunders since March 22, 2007. These emails and IM include conversations relating to Henry Saunders sending Roberta Harouff more counterfeit checks to be distributed throughout the United States. Saunders has attempted to send Harouff multiple packages the contained counterfeit monetary instruments but all of those packages were stopped by Affiant before they reached Harouff.

25. On April 19, 2007, Henry Saunders sent an email to Roberta Harouff utilizing the email account henrysaunders2004@yahoo.co.uk. The email contained 53 different names and addresses that Sanders instructed Harouff by IM to send counterfeit checks.

26. On July 10, 2007, United States Magistrate Judge Paul Stickney of the Northern District of Texas, issued a search warrant for the email account of jane_timi_jane@yahoo.com, to conduct a search for violations of Title 18, United States Code 523, Counterfeit Securities of the States and Private Entities. It was discovered through the investigation that an individual known as David Mark uses the email account jane_timi_jane@yahoo.com. The search of that email account revealed that David Mark was distributing counterfeit monetary instruments in the same manner as Henry Saunders.

27. A review of the email account jane_timi_jane@yahoo.com revealed that on May 19, 2007, Henry Saunders, utilizing the email account henrysaunders2004@yahoo.co.uk, sent David Mark an email with the subject line of "i beg wamart rebound 7k." The email contained one name, Nicholas Whalen, and an address of 1612 Worcester Rd., Apt. 309-A, Framingham,

Massachusetts. In my experience in this investigation, a "rebound" refers to sending a second or third set of checks to an individual who has already received checks and was successful in cashing the checks. The object of the rebound is to get the individual to cash as many checks as possible before that person or the bank realizes that the checks are counterfeit.

28. On May 21, 2007, David Mark, utilizing the email account jane_timi_jane@yahoo.com, sent an email to Shirley Johnson, at the email account caspergirl2u@yahoo.com, and entitled "ALL THE JOBS". That email contained a list of 52 names and addresses, including Nicolas Whalen. Typed besides Nicholas Whalen's name was "wallmart moneygram 7 pieces". On May 22, 2007, Johnson sent an email to David Mark listing 19 of the 52 names along with a UPS tracking number beside each name. The tracking number for Nicholas Whalen was a3613544912.

29. A search of the tracking number a3613544912 on UPS.com revealed that the package was dropped off for delivery on May 22, 2007 but the package was never sent. The remarks for the package read: "PKG DELAY-ADD'L SECURITY CHECK BY GOV'T OR OTHER AGENCY BEYOND UPS CONTROL / PACKAGE ABANDONED BY THE SENDER AND THE RECEIVER".

30. On October 6, 2007, Affiant contacted Nicholas Whalen and confirmed that, on or about May 15, 2007, he received a UPS package from an individual named Henry Saunders that contained 6 Ace Cash Express money gram money orders that were each in the amount of $490.00. Whalen stated that Henry Saunders offered him a work-at-home job over the internet. Whalen believed that he had entered into a legitimate business with Saunders, but later realized that it was a scam after he received the money orders, cashed them at his bank, wired money to

Kenya as instructed by Saunders, and then was informed by the bank that the money orders were counterfeit. Whalen stated that, because of the scam, he lost $2,645, plus bank fees.

31. The following is based upon Affiant's knowledge, training and experience, and the experience of other law enforcement personnel, including the information provided above regarding the internet:

a. Individuals who utilize the Internet can communicate by using email. E-mail usually contains a message header, containing information about the individual who originated a particular message or graphic, and importantly, the return address to respond to such individual.

b. Individuals who have an Internet e-mail address typically have a subscription to, membership, or affiliation with, an organization or commercial service, which provides access to the Internet computer network, known as an ISP. One such ISP is Yahoo, an Internet Service Provider, located at 701 First Avenue, Sunnyvale, California.

c. Internet Service Providers reserve and or maintain computer disk storage space on their computer system for the use of the Internet service subscribers for the storage of electronic communications with other parties (email), which include graphic files, programs, or other types of data stored in electronic form.

d. ISPs maintain records pertaining to the individuals or companies that are subscribers; ISPs maintain subscriber accounts that could include: credit card and other billing information, account access information, e-mail transaction information, news group access and posting information, account application information, and other information both in computer data format, and in written

record format, that record the activities and interactions of these accounts with the Internet or other materials relating to the subscribers' use of the ISP.

32. Based on previous investigations, and communication with Yahoo, the Affiant knows that Yahoo.co.uk is hosted by Yahoo, located at 701 First Avenue, Sunnyvale, California. Affiant has learned that Yahoo, as the host of all "yahoo.co.uk" services, is the central repository for all data, including messages, sent and received by that service.

CONCLUSION

Based on the foregoing, I believe that there is probable cause to believe that fruits, instrumentalities and evidence of Title 18, United States Code § 500, Counterfeit Money Orders, and § 513, Counterfeit Securities of the States and Private Entities, set forth in detail in Attachment B, will be found at the subject premises, described in Attachment A. As outlined above, one or more persons purporting to be Henry Saunders and/or De Mel Hiranya has engaged in a continuing scheme to counterfeit money orders and traveler's checks and to procure the services of others by solicitations on the internet in order to obtain genuine currency through such fraudulent scheme.

ABSENCE OF PRIVACY PROTECTION ACT CONCERNS

Your affiant is unaware of any materials relating to First Amendment activities such as publishing materials which would implicate the protections of the Privacy Protection Act ("PPA"), 42 U.S.C. Section 2000aa. However, should it become known that PPA protected materials have been seized *incidentally* because they were commingled with contraband or materials subject to seizure, such materials will be segregated and not further searched, and copies of the non-PPA protected materials will be retained, and the PPA protected materials will be returned to the owner together with any related hardware which is not contraband.

EXECUTION OF WARRANT

Pursuant to Title 18, United States Code, Section 2703(g), the presence of an officer is not required for service or execution of a search warrant requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

Greg Christiansen
Special Agent
U.S. Immigration and Customs Enforcement

Subscribed and sworn to before me this 10 day of October, 2007, in Dallas, Texas.

PAUL D. STICKNEY
United States Magistrate Judge

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is Yahoo, an Internet Service Provider, located at 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized, constituting evidence, fruits, and instrumentalities of violations of Title 18, United States Code § 500, Counterfeit Money Orders, and § 513, Counterfeit Securities of the States and Private Entities, are as follows:

1. Any and all Yahoo accounts for henrysaunders2004@yahoo.co.uk, to include all email, histories, buddy lists, profiles, subscriber information, method of payment, and detailed billings records (log on & log off times).

2. All customer or subscriber account information for the subscriber(s) to henrysaunders2004@yahoo.co.uk, including any e-mail address(es) and all customer or subscriber account information for any additional accounts subscribed to by the same subscriber(s) as henrysaunders2004@yahoo.co.uk. For each such account or e-mail address, the information should include the subscriber's name, account, login name, address, telephone number or numbers, and any other information pertaining to the identity of the subscriber, including any billing information;

3. User connection logs for all accounts identified in paragraph 1 above from May 16, 2007, to the present date. User connection logs should contain connection time and date, disconnect time and date, method of connection to system, and data transfer volume; and

4. The contents of all messages including instant messages, e-mail messages and attachments, including all messages sent to or from the accounts identified in paragraph 1 at any time after May 16, 2007.